UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,871	02/09/2004	Brant L. Candelore	SNY-T5714.02	8806

24337 7590 01/17/2007
MILLER PATENT SERVICES
2500 DOCKERY LANE
RALEIGH, NC 27606

EXAMINER	
SCHNURR, JOHN R	
ART UNIT	**PAPER NUMBER**
2621	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/774,871	**Applicant(s)** CANDELORE ET AL.	
	Examiner John R. Schnurr	**Art Unit** 2621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/09/2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-57* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *See Continuation Sheet*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :10/30/2006, 07/24/2006, 04/25/2006, 01/30/2006, 11/10/2005, 10/28/2005, 08/22/2005, 07/29/2005, 06/03/2005, 03/15/2005, 11/03/2004, 04/26/2004.

DETAILED ACTION

1. This Office Action is in response to Application No. 10/774,871 filed 2/29/2004. Claims 1 – 57 are pending and have been examined.

2.. The information disclosure statements (IDS) submitted on 4/26/2004, 11/03/2004, 03/15/2005, 06/03/2005, 07/29/2005, 08/22/2005, 10/28/2005, 11/10/2005, 01/30/2006, 04/25/2006, 07/24/2006, 10/30/2006 were considered by the examiner.

Claim Objections

3. Claims **37, 38, 39 and 40** are objected to because of the following informalities: Each of the claims, 37, 38, 39 and 40, are written to be dependent from claim 37. The claims should be dependent upon claim 36. During examination it was interpreted as if these claims were dependent upon claim 36. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

    1. Determining the scope and contents of the prior art.
    2. Ascertaining the differences between the prior art and the claims at issue.
    3. Resolving the level of ordinary skill in the pertinent art.
    4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims **1, 2, 3, 4, 5, 7, 8, 9, 10, 13, 14, 16, 18, 19, 20, 23, 24, 25, 26, 27, 29, 31, 32, 33, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49, 50 and 51** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iwamura (US Patent Application Publication 2003/0059047)** in view of **Bonan et al. (US Patent Application Publication 2004/0240668)**.

7. Claims **1, 2, 3, 4, 5, 7, 8, 9, 10, 13, 14, 16, 18, 19, 20, 23, 24, 25, 26, 27, 29, 31, 32, 33, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49, 50 and 51** are provisionally rejected under 35 U.S.C. 103(a) as being obvious over copending Application No. 10/767,421 which has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the copending application, it would constitute prior art under 35 U.S.C. 102(e) if published or patented. This provisional rejection under 35 U.S.C. 103(a) is based upon a presumption of future publication or patenting of the conflicting application.

This provisional rejection might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the copending application was derived from the inventor of this application and is thus not the invention “by another,” or by a showing of a date of invention for the instant application prior to the effective U.S. filing date of the copending application under 37 CFR 1.131. This rejection might also be overcome by showing that the copending application is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

Consider **claim 1,** Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A method of manipulating a stream of data in a CableCARD device, comprising:
>
> receiving a stream of data from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the stream of data comprising a plurality of packets each having a packet identifier (PID) associated therewith **(Fig. 2: Host CPU 250 informs CPU 270 of the PID (Packet Identifier) numbers of the program the user choses. [0066] Iwamura)**
>
> sending the data stream with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach the use of selective encryption via PID remapping. Specifically, Iwamura et al. do not teach:

> selecting certain of the packets for remapping of the packet identifiers associated with the selected packets;
> remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier;

In the same field of endeavor Bonan et al., which discloses a system for providing selective encryption on a set-top box (STB), clearly teaches;

> selecting certain of the packets for remapping of the packet identifiers associated with the selected packets;
> remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier; **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included selective encryption via PID remapping, as taught by Bonan et al., in the system disclosed by Iwamura for the advantage of allowing legacy equipment and encrypted equipment to operate in the same network (see paragraphs 48 to 50 of Bonan et al.) while providing the increased security benefits of a removable module.

Consider **claim 2**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 1, wherein the stream of data includes encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 3**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 2, wherein the stream of data is selectively encrypted. **(In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. [0056] Bonan)**

Consider **claim 4**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 2, further comprising decrypting the encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 5**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 4, further comprising re-encrypting the encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 and re-encrypted by encrypter 214. [0060] Iwamura)**

Consider **claim 7**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 4, wherein the remapping is carried out on the unencrypted packets. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 8**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 1, wherein the CableCARD comprises an OpenCable.TM. compliant CableCARD **(While the present invention is described in conjunction with an embodiment of an OpenCable.TM. compliant television Set-Top Box [0050] Iwamura)**

Consider **claim 9**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 1, wherein the remapping comprises remapping packets to substitute packets in the stream of data on a packet for packet basis. **(The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). [0074] Bonan)**

Consider **claim 10**, Iwamura combined with Bonan et al. as in claim 1, clearly teaches;

> The method according to claim 1, wherein the remapping comprises remapping packets to provide for insertion of a packet into the stream of data. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 13**, Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A method of manipulating a stream of data in a CableCARD device, comprising:
>
> receiving a stream of data from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the stream of data comprising a plurality of packets each having a packet identifier (PID) associated therewith **(Fig. 2: Host CPU 250 informs CPU 270 of the PID (Packet Identifier) numbers of the program the user choses. [0066] Iwamura)**, and wherein the stream of data further comprises encrypted packets **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**;
>
> decrypting the encrypted packets; **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**
>
> re-encrypting the decrypted packets . **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 and re-encrypted by encrypter 214. [0060] Iwamura)**; and
>
> sending the data stream with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach the use of selective encryption via PID remapping. Specifically, Iwamura et al. do not teach:

> selecting certain of the packets for remapping of the packet identifiers associated with the selected packets; remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier;

In the same field of endeavor Bonan et al., which discloses a system for providing selective encryption on a set-top box (STB), clearly teaches;

> selecting certain of the packets for remapping of the packet identifiers associated with the selected packets; remapping the packet identifiers of

> the selected packets so that the packets are associated with a new packet identifier; **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included selective encryption via PID remapping, as taught by Bonan et al., in the system disclosed by Iwamura for the advantage of allowing legacy equipment and encrypted equipment to operate in the same network (see paragraphs 48 to 50 of Bonan et al.) while providing the increased security benefits of a removable module.

Consider **claim 14**, Iwamura combined with Bonan et al. as in claim 13, clearly teaches;

> The method according to claim 13, wherein the stream of data is selectively encrypted. **(In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. [0056] Bonan)**

Consider **claim 16**, Iwamura combined with Bonan et al. as in claim 13, clearly teaches;

> The method according to claim 13, wherein the remapping is carried out after the decrypting. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 18**, Iwamura combined with Bonan et al. as in claim 13, clearly teaches;

> The method according to claim 13, wherein the CableCARD comprises an OpenCable.TM. compliant CableCARD. **(While the present invention is described in conjunction with an embodiment of an OpenCable.TM. compliant television Set-Top Box [0050] Iwamura)**

Consider **claim 19**, Iwamura combined with Bonan et al. as in claim 13, clearly teaches;

> The method according to claim 13, wherein the remapping comprises remapping packets to substitute packets in the stream of data on a packet

> for packet basis. **(The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). [0074] Bonan)**

Consider **claim 20**, Iwamura combined with Bonan et al. as in claim 13, clearly teaches;

> The method according to claim 13, wherein the remapping comprises remapping packets to provide for insertion of a packet into the stream of data. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 23**, Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A CableCARD device for manipulation of a stream of data, comprising:
>
> means for receiving a stream of data from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the stream of data comprising a plurality of packets each having a packet identifier (PID) associated therewith; **(Fig. 2: Host CPU 250 informs CPU 270 of the PID (Packet Identifier) numbers of the program the user choses. [0066] Iwamura)**
>
> means for sending the data stream with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach the use of selective encryption via PID remapping. Specifically, Iwamura et al. do not teach:

> a PID remapper that selects certain of the packets for remapping of the packet identifiers associated with the selected packets, and remaps the packet identifiers of the selected packets so that the packets are associated with a new packet identifier;

In the same field of endeavor Bonan et al., which discloses a system for providing selective encryption on a set-top box (STB), clearly teaches;

> a PID remapper that selects certain of the packets for remapping of the packet identifiers associated with the selected packets, and remaps the packet identifiers of the selected packets so that the packets are associated with a new packet identifier; **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included selective encryption via PID remapping, as taught by Bonan et al., in the system disclosed by Iwamura for the advantage of allowing legacy equipment and encrypted equipment to operate in the same network (see paragraphs 48 to 50 of Bonan et al.) while providing the increased security benefits of a removable module.

Consider **claim 24,** Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 23, wherein the stream of data further comprises encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 25**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 24, further comprising a decrypter for decrypting the encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 26**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 25, further comprising an encrypter for re-encrypting the decrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 and re-encrypted by encrypter 214. [0060] Iwamura)**

Consider **claim 27**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 24, wherein the stream of data is selectively encrypted. **(In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. [0056] Bonan)**

Consider **claim 29**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 23, wherein the remapping is carried out prior to the re-encrypting. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 31**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 23, wherein the CableCARD comprises an OpenCable.TM. compliant CableCARD. **(While the present invention is described in conjunction with an embodiment of an OpenCable.TM. compliant television Set-Top Box [0050] Iwamura)**

Consider **claim 32**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 23, wherein the remapping comprises remapping packets to substitute packets in the stream of data on a packet for packet basis. **(The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). [0074] Bonan)**

Consider **claim 33**, Iwamura combined with Bonan et al. as in claim 23, clearly teaches;

> The CableCARD device according to claim 23, wherein the remapping comprises remapping packets to provide for insertion of a packet into the stream of data. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 36**, Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A CableCARD device for manipulation of a stream of data, comprising:
>
> means for receiving a stream of data from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the stream of data comprising a plurality of packets each having a packet identifier (PID) associated therewith; **(Fig. 2: Host CPU 250 informs CPU 270 of the PID (Packet Identifier) numbers of the program the user choses. [0066] Iwamura)**
>
> means for sending the data stream with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach the use of selective encryption via PID remapping. Specifically, Iwamura et al. do not teach:

> a PID remapper that selects certain of the packets for remapping of the packet identifiers associated with the selected packets, and remaps the packet identifiers of the selected packets so that the packets are associated with a new packet identifier;

In the same field of endeavor Bonan et al., which discloses a system for providing selective encryption on a set-top box (STB), clearly teaches;

> a PID remapper that selects certain of the packets for remapping of the packet identifiers associated with the selected packets, and remaps the packet identifiers of the selected packets so that the packets are associated with a new packet identifier; **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included selective encryption via PID remapping, as taught by Bonan et al., in the system disclosed by Iwamura for the advantage of allowing legacy equipment and encrypted equipment to operate in the same network (see paragraphs 48 to 50 of Bonan et al.) while providing the increased security benefits of a removable module.

Consider **claim 37**, Iwamura combined with Bonan et al. as in claim 36, clearly teaches;

> The CableCARD device according to claim 37, wherein the stream of data is selectively encrypted. **(In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. [0056] Bonan)**

Consider **claim 38**, Iwamura combined with Bonan et al. as in claim 36, clearly teaches;

> The CableCARD device according to claim 37, wherein the remapping is carried out at any point prior to the decrypting, prior to the re-encrypting **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**, or after the re-encrypting.

Consider **claim 39**, Iwamura combined with Bonan et al. as in claim 36, clearly teaches;

> The CableCARD device according to claim 37, wherein the CableCARD comprises an OpenCable.TM. compliant CableCARD. **(While the present invention is described in conjunction with an embodiment of an OpenCable.TM. compliant television Set-Top Box [0050] Iwamura)**

Consider **claim 40**, Iwamura combined with Bonan et al. as in claim 36, clearly teaches;

> The CableCARD device according to claim 37, wherein the remapping comprises remapping packets in at least one of the following manners:
>
> remapping packets to substitute packets in the stream of data on a packet for packet basis; **(The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). [0074] Bonan)**
>
> remapping packets to provide for insertion of a packet into the stream of data;

> remapping one packet for multiple packets; or mapping multiple packets for one packet.

Consider **claim 41**, Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A method of manipulating a stream of data in a CableCARD device, comprising:
>
> receiving a stream of data from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the stream of data comprising a plurality of packets each having a packet identifier (PID) associated therewith; **(Fig. 2: Host CPU 250 informs CPU 270 of the PID (Packet Identifier) numbers of the program the user choses. [0066] Iwamura)**
>
> •
>
> sending the data stream with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach the use of selective encryption via PID remapping. Specifically, Iwamura et al. do not teach:

> selecting certain of the packets for remapping of the packet identifiers associated with the selected;

In the same field of endeavor Bonan et al., which discloses a system for providing selective encryption on a set-top box (STB), clearly teaches;

> selecting certain of the packets for remapping of the packet identifiers associated with the selected packets **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**;

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included selective encryption via PID remapping, as taught by Bonan et al., in the system disclosed by Iwamura for the advantage of allowing legacy equipment and encrypted equipment to operate in the same network (see paragraphs 48 to 50 of Bonan et al.) while providing the increased security benefits of a removable module.

Consider **claim 42**, Iwamura combined with Bonan et al. as in claim 41, clearly teaches;

> The method according to claim 41, wherein the stream of data includes encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 43**, Iwamura combined with Bonan et al. as in claim 42, clearly teaches;

> The method according to claim 42, wherein the stream of data is selectively encrypted. **(In general, the encryption technique disclosed herein seeks to encrypt portions of an audio or video signal while leaving other portions of the audio or video signal in the clear to conserve bandwidth. [0056] Bonan)**

Consider **claim 44**, Iwamura combined with Bonan et al. as in claim 42, clearly teaches;

> The method according to claim 42, further comprising decrypting the encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 [0060] Iwamura)**

Consider **claim 45**, Iwamura combined with Bonan et al. as in claim 44, clearly teaches;

> The method according to claim 44, further comprising re-encrypting the encrypted packets. **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 and is decrypted by decrypter 218 and re-encrypted by encrypter 214. [0060] Iwamura)**

Consider **claim 47**, Iwamura combined with Bonan et al. as in claim 44, clearly teaches;

> The method according to claim 44, further comprising remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier, wherein the remapping is carried out on the unencrypted packets. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the**

> **data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 48**, Iwamura combined with Bonan et al. as in claim 41, clearly teaches;

> The method according to claim 41, wherein the CableCARD comprises an OpenCable.TM. compliant CableCARD. **(While the present invention is described in conjunction with an embodiment of an OpenCable.TM. compliant television Set-Top Box [0050] Iwamura)**

Consider **claim 49**, Iwamura combined with Bonan et al. as in claim 41, clearly teaches;

> The method according to claim 41, further comprising remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

Consider **claim 50**, Iwamura combined with Bonan et al. as in claim 49, clearly teaches;

> The method according to claim 49, further comprising remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier, wherein the remapping comprises remapping packets to substitute packets in the stream of data on a packet for packet basis. **(The primary PIDs (025) in the input stream are replaced with the secondary PID (125) for the clear packets (C). [0074] Bonan)**

Consider **claim 51**, Iwamura combined with Bonan et al. as in claim 49, clearly teaches;

> The method according to claim 49, wherein the remapping comprises remapping packets to provide for insertion of a packet into the stream of data. **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

8. Claims **11, 12, 21, 22, 34, 35, 52 and 53** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iwamura (US Patent Application Publication 2003/0059047)** in view of **Bonan et al. (US Patent Application Publication 2004/0240668)** as applied to claims 1, 13, 23 and 41 above, and further in view of **Ryal (US Patent Application Publication 2005/0066357)**.

9. Claims **11, 12, 21, 22, 34, 35, 52 and 53** are provisionally rejected under 35 U.S.C. 103(a) as being obvious over copending Application No. 10/767,421 which has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the copending application, it would constitute prior art under 35 U.S.C. 102(e) if published or patented. This provisional rejection under 35 U.S.C. 103(a) is based upon a presumption of future publication or patenting of the conflicting application.

This provisional rejection might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the copending application was derived from the inventor of this application and is thus not the invention "by another," or by a showing of a date of invention for the instant application prior to the effective U.S. filing date of the copending application under 37 CFR 1.131. This rejection might also be overcome by showing that the copending application is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

Consider **claim 11**, Iwamura combined with Bonan et al. as in claim 1 clearly teaches the use of a PID remapping.

> The method according to claim 1, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 1 does not explicitly teach the remapping technique of mapping one packet for multiple packets. Specifically, Iwamura et al. do not teach:

> remapping comprises mapping one packet for multiple packets.

In the same field of endeavor Ryal, which discloses a system for modifying content rating of a program by substituting content, clearly teaches;

> remapping comprises mapping one packet for multiple packets. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the one for many packet remapping, as taught by Ryal, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of being able to replace objectionable material in a program with non-objectionable material (see paragraph 2 of Ryal).

Consider **claim 12**, Iwamura combined with Bonan et al. further combined with Ryal as in claim 11, clearly teaches;

> The method according to claim 1, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)** comprises mapping multiple packets for one packet. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the**

> **main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Consider **claim 21**, Iwamura combined with Bonan et al. as in claim 13 clearly teaches the use of a PID remapping.

> The method according to claim 13, wherein the remapping **Fig. 2: (Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 1 does not explicitly teach the remapping technique of mapping one packet for multiple packets. Specifically, Iwamura et al. do not teach:

> remapping comprises mapping one packet for multiple packets.

In the same field of endeavor Ryal, which discloses a system for modifying content rating of a program by substituting content, clearly teaches;

> remapping comprises mapping one packet for multiple packets. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the one for many packet remapping, as taught by Ryal, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of being able to replace objectionable material in a program with non-objectionable material (see paragraph 2 of Ryal).

Consider **claim 22**, Iwamura combined with Bonan et al. further combined with Ryal as in claim 21, clearly teaches;

> The method according to claim 13, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)** comprises mapping multiple packets for one packet. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at**

> **342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Consider **claim 34**, Iwamura combined with Bonan et al. as in claim 23 clearly teaches the use of a PID remapping.

> The CableCard device according to claim 23, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 23 does not explicitly teach the remapping technique of mapping one packet for multiple packets. Specifically, Iwamura et al. do not teach:

> remapping comprises mapping one packet for multiple packets.

In the same field of endeavor Ryal, which discloses a system for modifying content rating of a program by substituting content, clearly teaches;

> remapping comprises mapping one packet for multiple packets. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the one for many packet remapping, as taught by Ryal, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of being able to replace objectionable material in a program with non-objectionable material (see paragraph 2 of Ryal).

Consider **claim 35**, Iwamura combined with Bonan et al. further combined with Ryal as in claim 34, clearly teaches;

> The CableCARD device according to claim 23, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)** comprises mapping multiple packets for one packet. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content**

> **is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Consider **claim 52**, Iwamura combined with Bonan et al. as in claim 49 clearly teaches the use of a PID remapping.

> The method according to claim 49, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 49 does not explicitly teach the remapping technique of mapping one packet for multiple packets. Specifically, Iwamura et al. do not teach:

> remapping comprises mapping one packet for multiple packets.

In the same field of endeavor Ryal, which discloses a system for modifying content rating of a program by substituting content, clearly teaches;

> remapping comprises mapping one packet for multiple packets. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the one for many packet remapping, as taught by Ryal, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of being able to replace objectionable material in a program with non-objectionable material (see paragraph 2 of Ryal).

Consider **claim 53**, Iwamura combined with Bonan et al. further combined with Ryal as in claim 52, clearly teaches;

> The method according to claim 49, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)** comprises mapping multiple packets for one packet. **(Fig. 3: If, however, the**

> **replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

10. Claims **6, 15, 17, 28, 30 and 46** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iwamura (US Patent Application Publication 2003/0059047)** in view of **Bonan et al. (US Patent Application Publication 2004/0240668)** as applied to claims 1, 13, 23 and 41 above, and further in view of **Pinder et al. (US Patent Application Publication)**.

11. Claims **6, 15, 17, 28, 30 and 46** are provisionally rejected under 35 U.S.C. 103(a) as being obvious over copending Application No. 10/767,421 which has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the copending application, it would constitute prior art under 35 U.S.C. 102(e) if published or patented. This provisional rejection under 35 U.S.C. 103(a) is based upon a presumption of future publication or patenting of the conflicting application.

This provisional rejection might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the copending application was derived from the inventor of this application and is thus not the invention "by another," or by a showing of a date of invention for the instant application prior to the effective U.S. filing date of the copending application under 37 CFR 1.131. This rejection might also be overcome by showing that the copending application is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

Consider **claim 6**, Iwamura combined with Bonan et al. as in claim 1 clearly teaches the use of a PID remapping.

> The method according to claim 4, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 1 does not explicitly teach the remapping of PIDs on encrypted packets. Specifically, Iwamura et al. combined with Bonan et al. do not teach:

> the remapping is carried out on the encrypted packets.

In the same field of endeavor Pinder et al., which discloses a system for implementing a dual encrypted stream using two STBs, clearly teaches;

> the remapping is carried out on the encrypted packets. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the remapping of encrypted packets, as taught by Pinder, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of inserting encrypted data into a stream (see paragraph 39 of Pinder et al.).

Consider **claim 15**, Iwamura combined with Bonan et al. as in claim 13 clearly teaches the use of a PID remapping.

> The method according to claim 13, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 1 does not explicitly teach the remapping of PIDs on encrypted packets. Specifically, Iwamura et al. combined with Bonan et al. do not teach:

> wherein the remapping is carried out prior to the decrypting.

In the same field of endeavor Pinder et al., which discloses a system for implementing a dual encrypted stream using two STBs, clearly teaches;

> wherein the remapping is carried out prior to the decrypting. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the remapping of encrypted packets, as taught by Pinder, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of inserting encrypted data into a stream (see paragraph 39 of Pinder et al.).

Consider **claim 17**, Iwamura combined with Bonan et al. further combined with Pinder et al. as in claim 15, clearly teaches;

The method according to claim 13, wherein the remapping is carried out after the re-encrypting. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder) Encrypted packets are remapped.**

Consider **claim 28**, Iwamura combined with Bonan et al. as in claim 23 clearly teaches the use of a PID remapping.

> The CableCARD device according to claim 23, wherein the remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 23 does not explicitly teach the remapping of PIDs on encrypted packets. Specifically, Iwamura et al. combined with Bonan et al. do not teach:

> the remapping is carried out prior to the decrypting.

In the same field of endeavor Pinder et al., which discloses a system for implementing a dual encrypted stream using two STBs, clearly teaches;

> the remapping is carried out prior to the decrypting. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the remapping of encrypted packets, as taught by Pinder, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of inserting encrypted data into a stream (see paragraph 39 of Pinder et al.).

Consider **claim 30**, Iwamura combined with Bonan et al. further combined with Pinder et al. as in claim 28, clearly teaches;

> The CableCARD device according to claim 23, wherein the remapping is carried out after the re-encrypting. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder) Encrypted packets are remapped.**

Consider **claim 46**, Iwamura combined with Bonan et al. as in claim 23 clearly teaches the use of a PID remapping.

> The method according to claim 44, further comprising remapping **(Fig. 2: Encrypted packets with the secondary PID are decrypted at 230 and then recombined with the data stream (e.g., by remapping the packets to the primary PID) for decoding. [0064] Bonan)**

However, Iwamura combined with Bonan et al. as in claim 23 does not explicitly teach the remapping of PIDs on encrypted packets.· Specifically, Iwamura et al. combined with Bonan et al. do not teach:

> remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier, wherein the remapping is carried out on the encrypted packets.

In the same field of endeavor Pinder et al., which discloses a system for implementing a dual encrypted stream using two STBs, clearly teaches;

> remapping the packet identifiers of the selected packets so that the packets are associated with a new packet identifier, wherein the remapping is carried out on the encrypted packets. **(Fig. 7: The scrambler B 745 encrypts the packet of clear stream C according to a second encryption method and provides the encrypted packet to a PID remapper 750. The PID remapper 750 remaps the packet's PID value to a new PID value [0039] Pinder)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the remapping of encrypted packets, as taught by Pinder, in the system disclosed by Iwamura combined with Bonan et al. as in claim 1 for the advantage of inserting encrypted data into a stream (see paragraph 39 of Pinder et al.).

12. Claims **54 and 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iwamura (US Patent Application Publication 2003/0059047)** in view of **Coupe et al. (US Patent Application Publication 2006/0136976)**.

Consider **claim 54**, Iwamura clearly teaches the use of a removable device for the manipulation of a stream of data containing packet identifiers (PIDs).

> A method of manipulating a stream of data in a CableCARD device **(Fig. 2 POD 150)**, comprising:

> sending the first stream of data including the selected packets with remapped packet identifiers back to the host. **(Fig. 2: The re-encrypted data stream goes to decrypter 224 through the POD interface 212. [0060] Iwamura)**

The use of a removable device allows for improved security of data by manipulating data inside the device and transmitting encrypted data back to the host (see paragraph 7 of Iwamura).

However, Iwamura does not explicitly teach PID remapping of multiple transport streams.

> receiving first and second streams of data, the first and second streams of data comprising a plurality of packets each having a packet identifier (PID) associated therewith;

> selecting certain of the packets from the second stream of data for remapping of the packet identifiers associated with the selected packets;
>
> remapping the packet identifiers of the selected packets so that the packets are associated with a packet identifier that identifies the selected packets as being a part of the first stream

In the same field of endeavor Coupe et al., which discloses a system for remapping multiple transport streams, clearly teaches;

> receiving first and second streams of data **(Fig. 4: Receiver 100 receives two independent network inputs 101, 102 at separate network interfaces 103, 104, respectively. [0056] Coupe)** from a host **(Fig. 2: The data from the front-end 208 is thus diverted to the POD card 150 [0060] Iwamura)**, the first and second streams of data comprising a plurality of packets each having a packet identifier (PID) associated therewith **(Incoming packets would be filtered based on the PID values within the header of the packet. [0059] Coupe)**;
>
> selecting certain of the packets from the second stream of data for remapping of the packet identifiers associated with the selected packets **(All PIDs from the secondary stream needing to be reassigned, would then have a re-map value associated with them. [0059] Coupe)**;
>
> remapping the packet identifiers of the selected packets so that the packets are associated with a packet identifier that identifies the selected packets as being a part of the first stream **(Up to 32 re-maps would be possible, meaning the hardware would contain a bank of PID look-up entries and a corresponding bank of re-map values. Any PIDs with PID look-up entries would have the PID value within the header of the packet replaced with the re-map value before being forwarded to the transport demultiplexor. [0059] Coupe)**;

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included remapping of multiple transport streams, as taught by Coupe et al., in the system disclosed by Iwamura for the advantage of allowing multiple transport streams to be received and processed simultaneously (see paragraph 5 of Coupe et al.) while providing the increased security benefits of a removable module.

Consider **claim 55**, Iwamura combined with Coupe et al. as in claim 54, clearly teaches;

> The method according to claim 54, wherein the remapping comprises remapping packets to provide for insertion of a packet into the first stream of data. **(All PIDs from the secondary stream needing to be reassigned, would then have a re-map value associated with them. Up to 32 re-maps would be possible, meaning the hardware would contain a bank of PID look-up entries and a corresponding bank of re-map values. Any PIDs with PID look-up entries would have the PID value within the header of the packet replaced with the re-map value before being forwarded to the transport demultiplexor. [0059] Coupe)**

13. Claims **56 and 57** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iwamura (US Patent Application Publication 2003/0059047)** in view of **Coupe et al. (US Patent Application Publication 2006/0136976)** as applied to claim 54 above, and further in view of **Ryal (US Patent Application Publication 2005/0066357)**.

Consider **claim 56**, Iwamura combined with Coupe et al. as in claim 54 clearly teaches the use of a PID remapping.

> The method according to claim 54, wherein the remapping **(PID re-mapping: Incoming packets would be filtered based on the PID values within the header of the packet. Up to a total of 32 PIDs could be filtered from both streams. Packets matching the PID filter would be forwarded to the transport demultiplexor. All PIDs from the secondary stream needing to be reassigned, would then have a re-map value associated with them. Up to 32 re-maps would be possible, meaning the hardware would contain a bank of PID look-up entries and a corresponding bank of re-map values. Any PIDs with PID look-up entries would have the PID value within the header of the packet replaced with the re-map value before being forwarded to the transport demultiplexor. [0059] Coupe)**

However, Iwamura combined with Coupe et al. as in claim 54 does not explicitly teach the remapping technique of mapping one packet for multiple packets.

> remapping comprises mapping one packet for multiple packets.

In the same field of endeavor Ryal, which discloses a system for modifying content rating of a program by substituting content, clearly teaches;

> remapping comprises mapping one packet for multiple packets. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Therefore, at the time the invention was made, it would have been obvious to one with ordinary skill in the art to have included the one for many packet remapping, as taught by Ryal, in the system disclosed by Iwamura combined with Coupe et al. as in claim 54 for the advantage of being able to replace objectionable material in a program with non-objectionable material (see paragraph 2 of Ryal) while providing the increased security benefits of a removable module.

Consider **claim 57**, Iwamura combined with Coupe et al. further combined with Ryal as in claim 56, clearly teaches;

> The method according to claim 54, wherein the remapping comprises mapping multiple packets for one packet. **(Fig. 3: If, however, the replacement content is available at 328, the replacement content is retrieved at 338 and is used to replace the removed main content at 342. The PID of the replacement content is mapped to the PID of the main content at 346 and the content is sent to a decoder at 350 for play of the replacement content. [0029] Ryal)**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John R. Schnurr whose telephone number is (571) 270-1458. The examiner can normally be reached on Monday - Friday, 7:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Patrick Edouard can be reached on (571) 272-7603. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRS

PATRICK N. EDOUARD
SUPERVISORY PATENT EXAMINER